# TRAITE DE COOPERATION EN MATIERS DE BREVETS PCT

### RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

			essier du déposant ou du	DOUB SUITE A D	ONNED voir la notifica	ation de transmission du rapport d'examen					
mar	ndataire			POUR SUITE A DONNER volr la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)							
Demande internationale No.				Date du dépôt international (jour/mois/année)		Date de priorité (jour/mols/année)					
PC	T/FR	03/0	1535	21.05.2003		05.06.2002					
1			emationale des brevets (CIE	3) ou à la fois classification	n nationale et CIB						
H04L9/32											
Déposant											
FR	FRANCE TELECOM et al.										
1.											
	international, est transmis au déposant conformément à l'article 36.										
2.	. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.										
☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins o											
		ont	été modifiées et qui serv	ent de base au préser	it rapport ou de feuilles	contenant des rectifications faites (voir la règle 70.16 et l'instruction 607					
			Instructions administration		siiililaile iilleilialiollai	(voii la regie 70. 16 et l'instruction 607					
	Ces	anne	exes comprennent feuille	es.							
3.	Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :										
I ⊠ Base de l'opinion											
İ	П		Priorité								
	Ш		Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle								
	IV  Absence d'unité de l'invention										
V 🖾 Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la pos d'application industrielle; citations et explications à l'appui de cette déclaration					l'activité inventive et la possibilité déclaration						
	VI		Certains documents cit	tés							
VII 🔲 Irrégularités dans la demande internationale											
	VIII		Observations relatives	à la demande internat	ionale						
Date de présentation de la demande d'examen préliminaire					Date d'achèvement du	présent rapport					
interr	nationa	ıle									
19.1	2.200	03			10.11.2004						
Nom	et adre	9880 1	oostale de l'adminstration ch	argée de l'examen	Fonctionnaire autorisé						
		interr	national	-	. Silodoffilano autorise	Conference Patrone					
	(III)	NL	ice européen des brevets - I -2280 HV Rijswijk - Pays Ba	ıs	Holper, G						
Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016					N° de téléphone +31 70	340-2304					

# RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n°

PCT/FR 03/01535

1. En ce qui concerne les éléments de la demande internationale (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)):

	Description, Pages								
	1-1	3	telles qu'initialement déposées						
	Re	vendications, No.							
	1-1	4	telles qu'initialement déposées						
	Des	ssins, Feuilles							
	1/3-	-3/3	telles qu'initialement déposées						
2.	ou	ce qui concerne la <b>la</b> lui ont été remis dans traire donnée sous c	ngue, tous les éléments indiqués ci-dessus étaient à la disposition de l'administrations la langue dans laquelle la demande internationale a été déposée, sauf indication e point.	า					
	Ces	Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est:							
		la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).							
		la langue de publica	tion de la demande internationale (selon la règle 48.3(b)).						
		la langue de la tradu 55.3).	uction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou						
3.	inte	ce qui concerne les <b>séquences de nucléotides ou d'acide aminés</b> divulguées dans la demande ernationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des juences :							
	☐ contenu dans la demande internationale, sous forme écrite.								
		déposé avec la demande internationale, sous forme déchiffrable par ordinateur.							
		remis ultérieurement	emis ultérieurement à l'administration, sous forme écrite.						
		remis ultérieurement	t à l'administration, sous forme déchiffrable par ordinateur.						
		La déclaration, selor de la divulgation fait	n laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-del le dans la demande telle que déposée, a été fournie.	à					
La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sor à celles du listages des séquences Présenté par écrit, a été fournie.									
4.	Les	s modifications ont entraîné l'annulation :							
		de la description,	pages:						
		des revendications,	nos:						
		des dessins,	feuilles:						

## RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n°

1-14

PCT/FR 03/01535

5. Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)):

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

- 6. Observations complémentaires, le cas échéant :
- V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- 1. Déclaration

Nouveauté Oui: Revendications

Non: Revendications

Activité inventive Oui: Revendications 3-7, 9

Non: Revendications 1,2,8,10-14

Possibilité d'application industrielle Oui: Revendications 1-14

Non: Revendications

2. Citations et explications

voir feuille séparée

### Concernant le point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence aux documents suivants :

D1: US-B-6 215 872 B1 (VAN OORSCHOT PAUL C) 10 avril 2001 (2001-04-10)

D2: EP-A-0 856 821 (NIPPON TELEGRAPH & TELEPHONE) 5 août 1998 (1998-08-

05)

La présente demande ne remplit pas les conditions énoncées dans l'article 33(1) PCT, l'objet des revendications 1,2, 8, 11-14 n'impliquant pas une activité inventive telle que définie par l'article 33(3) PCT.

Le document D1, qui est considéré comme étant l'état de la technique le plus proche de l'objet de la revendication 1, décrit (voir col.4, l.11-42; col.5, l.2-5; col.8, l.60 - col.9, I.12; les références entre parenthèses s'appliquent à ce document) : un procédé de vérification d'une signature électronique, faisant intervenir un utilisateur comprenant un système de traitement de données, l'utilisateur recevant du système de traitement de données, des demandes de vérification de signatures électroniques et traitant ces demandes, une signature électronique étant générée à l'aide d'une clé privée connue seulement d'une entité signataire et associée à une clé publique, comprenant une étape de stockage dans une table de certificats (trusted public key list 36) contenant une forme condensée d'au moins une clé publique, et une phase de vérification d'une signature électronique comportant les étapes consistant à : - recevoir la signature électronique à vérifier et une clé publique d'une paire de clés comprenant une clé privée ayant été utilisée pour générer la signature électronique à vérifier, calculer une forme condensée de la clé publique reçue, et rechercher dans la table de certificats (36) la forme condensée calculée de la clé publique, et - déchiffrer la signature électronique à l'aide de la clé publique reçue si la forme condensée calculée de la clé publique se trouve dans la table de certificats.

Par conséquent, l'objet de la revendication 1 diffère de ce procédé connu uniquement en ce que le procédé fait intervenir un microcircuit connectable à un système de traitement de données et en ce que la table de certificats est stockée dans une mémoire du microcircuit.

Le problème que se propose de résoudre la présente invention comme définie par la revendication 1 peut donc être considéré comme étant la réalisation pratique du procédé connu.

Toutefois il est connu de stocker des certificats et des clés publiques dans une

mémoire d'une carte à puce (voir D2, fig.4B, col.5, l.57 - col.6, l.29). L'homme de l'art utiliserait sûrement une telle carte pour réaliser le procédé selon D1 et arriverait ainsi à l'objet de la revendication 1 sans exercer une activité inventive.

Le même argument s'applique mutatis mutandis à l'objet des revendications indépendantes correspondantes 13 et 14 qui ne sont donc pas non plus inventives.

La revendication dépendante 2 ne contient aucune caractéristique additionnelle qui en combinaison avec la recendication 1, définisse un objet qui satisfasse aux exigences de l'article 33(3) PCT pour la raison suivante:

les étapes supplémentaires mentionnées sont équivalentes à une vérification classique d'un certificat recu; l'homme de l'art effectuerait cette procédure avant l'insertion d'une clé publique ou de son condensé afin de garantir l'authenticité du certificat reçu et arriverait ainsi à la matière de la revendication 2 sans exercer une activité inventive.

Les revendications dépendantes 8, 10, 11 et 12 ne contiennent aucune caractéristique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences du PCT en ce qui concerne l'activité inventive, voir documents D1 et D2 et les passages correspondants cités dans le rapport de recherche.

La combinaison des caractéristiques de la revendication 3 n'est pas comprise dans l'état de la technique et n'en découle pas de manière évidente pour les raisons suivantes : aucun document de l'art antérieur ne divulgue l'insertion d'un pointeur vers le condensé de la clé publique de l'entité de certification ayant émis un certificat, définissant ansi un arbre de certification stocké dans une mémoire d'un microcircuit,. La combinaison des caractéristiques de la revendication 9 n'est pas non-plus comprise dans l'état de la technique et n'en découle pas de manière évidente. La revendications 3 et 9 remplissent donc les critères de l'article 33(2) et (3) du PCT.

Les revendications 4 - 6, en supposant qu'elles dépendent de la revendication 3, satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D1 et D2 et ne cite pas ces documents.